



DJ-CERT

Centre national de veille,
d'alerte et de réponse aux
attaques informatiques

Autorité Nationale de Cybersécurité

Djibouti le, 21-10-2026

BULLETIN ALERTES

Object	Vulnérabilités critiques PHP2Shell dans PHP (CVE-2026-109618 & CVE-2026-109619)
Référence	1507
Date de Publication	2026-10-21
Sévérité	Critique

IMPACT :

- Exécution de code arbitraire à distance (RCE) sans authentification, avec les privilèges du compte du serveur web ;
- Corruption de la mémoire lors d'un épuisement de mémoire (OOM) pendant le traitement d'une requête (CVE-2026-109618) ;
- Utilisation après libération (use-after-free) d'un état global conservé entre deux requêtes traitées par le même processus (CVE-2026-109619), pouvant aussi entraîner une divulgation de mémoire ;
- Dépôt de webshells, vol de données et prise de contrôle du serveur ;
- Atteinte à la confidentialité, à l'intégrité et à la disponibilité des données.

SYSTÈME AFFECTÉ :

- Toute installation PHP traitant des requêtes web : PHP-FPM, Apache avec mod_php, php-cgi, FrankenPHP et LiteSpeed (risque le plus élevé avec mod_php) ;
- Branches soutenues : versions antérieures à PHP 8.2.35, 8.3.36, 8.4.27 et 8.5.12 ;
- PHP 8.1 et versions antérieures (8.0, 7.x, 5.x) : fin de vie, aucune mise à jour officielle ;
- Versions corrigées (publiées le 21 octobre 2026) : PHP 8.2.35, 8.3.36, 8.4.27 et 8.5.12



DÉSCRIPTION :

Deux vulnérabilités critiques d'exécution de code à distance, surnommées « PHP2Shell », ont été corrigées le 21 octobre 2026 par l'équipe de sécurité de PHP. Référencées CVE-2026-109618 et CVE-2026-109619, elles se situent dans le cœur

du langage PHP, et non dans une application ou un CMS particulier. Chacune est évaluée à 9,2 sur 10 selon l'échelle CVSS v4.0. Les détails ont fuité le 20 octobre, avant la divulgation coordonnée, ce qui a conduit PHP à avancer la publication des correctifs.

CVE-2026-109618 (RCE via corruption lors d'un OOM) : lorsque PHP manque de mémoire, il interrompt brutalement le traitement de la requête alors que certaines données internes ne sont que partiellement initialisées. La procédure de fin de requête traite ensuite ces données invalides comme valides. Plusieurs techniques liées à l'analyse des requêtes multipart permettent à un attaquant de provoquer cet épuisement de mémoire de façon fiable. Avec Apache mod_php, l'attaque aboutit avant l'exécution de tout code applicatif ; une exécution de code complète a été validée avec les limites PHP par défaut.

CVE-2026-109619 (RCE via un état global obsolète) : certains états globaux (erreurs, session, objets, extensions) conservés par un processus PHP peuvent continuer à pointer vers la mémoire d'une requête déjà libérée. Une requête suivante traitée par le même processus peut utiliser cet état avant sa réinitialisation (use-after-free). Deux cas sont confirmés : la fonctionnalité session.upload_progress (activée par défaut, sans appel à session_start()), validée sur mod_php et PHP-FPM, et l'option fatal_error_backtraces de PHP 8.5, validée sur mod_php.

Selon l'avis officiel, l'exploitation ne nécessite pas de faille d'inclusion de fichier local (LFI) dans l'application. Les chercheurs indiquent que toutes les versions depuis PHP 5.4.0 seraient concernées ; l'avis officiel ne fixe pas de borne inférieure. Un outil d'exploitation et des analyses techniques sont publics. Sansec rapporte que Cloudflare a observé de premières attaques le 21 octobre et anticipe une exploitation massive. Selon Mallory (données Shodan du 20 octobre), environ 1,5 million d'hôtes exposés sur Internet affichent leur version de PHP, dont près de 884 000 (environ 59%) sous PHP 8.1 ou antérieur, sans correctif officiel.

SOLUTION :

Mettre à jour PHP vers la version 8.5.12, 8.4.27, 8.3.36 ou 8.2.35 selon la branche utilisée, et se référer au bulletin de sécurité officiel de PHP (voir la rubrique Documentation)

DOCUMENTATION :

- Avis de sécurité officiel PHP (21 octobre 2026) :
<https://www.php.net/archive/2026.php#2026-10-21-5>
- Avis GitHub PHP – CVE-2026-109618 (GHSA-w8hw-w9fx-j79w) :
<https://github.com/php/php-src/security/advisories/GHSA-w8hw-w9fx-j79w>
- Avis GitHub PHP – CVE-2026-109619 (GHSA-6wmf-4rv5-p3rp) :
<https://github.com/php/php-src/security/advisories/GHSA-6wmf-4rv5-p3rp>
- Téléchargement des versions corrigées :
<https://www.php.net/downloads.php>
- Références CVE (NVD) :

<https://nvd.nist.gov/vuln/detail/CVE-2026-109618>

<https://nvd.nist.gov/vuln/detail/CVE-2026-109619>

- Bulletin Huntress Rapid Response (21 octobre 2026) :
<https://www.huntress.com/blog/php2shell-leaked-critical-php-vulnerabilities>
- Analyse Sansec (21 octobre 2026) :
<https://sansec.io/research/php2shell>
- FAQ watchTowr (20 octobre 2026, mise à jour le 21) :
<https://watchtowr.com/intelligence/php-cve-2026-109618-faq>
- Article CyberSecurity News (21 octobre 2026) – dépôt PoC non officiel :
<https://cybersecuritynews.com/php2shell-vulnerability/>
- Catalogue CISA Known Exploited Vulnerabilities (KEV) :
<https://www.cisa.gov/known-exploited-vulnerabilities-catalog>